Design Methodology for Safe & Arm Devices

Dipl.-Phys. Friedrich Sauerländer

Who am I?

NAWC WPNS
Ordnance Systems Division
China Lake, CA

BWB
WF I 5
Koblenz, Germany

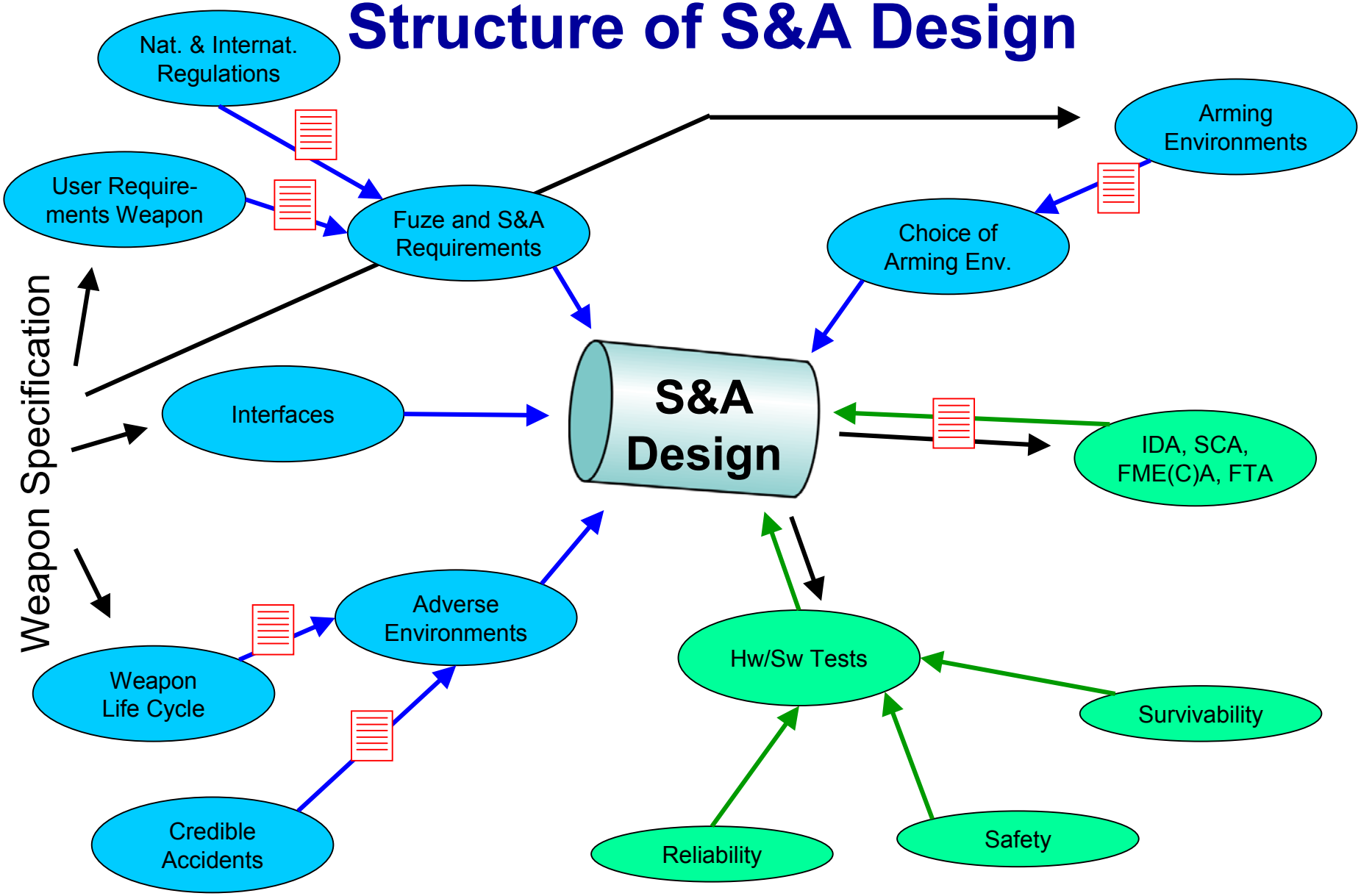
Outline

- **S&A Development Process**
  - Steps to a safe S&A
- **Fault Tree Analysis**
  - How to do it right

Full Report available from: FowlerSE@navair.navy.mil

Where to start?

Structure of S&A Design



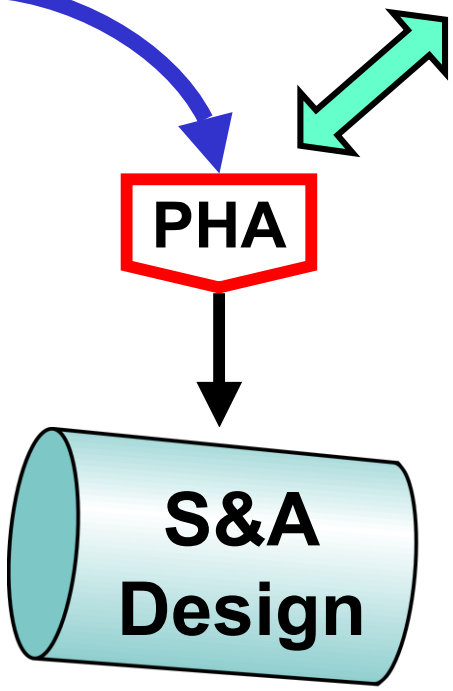
S&A Design Process

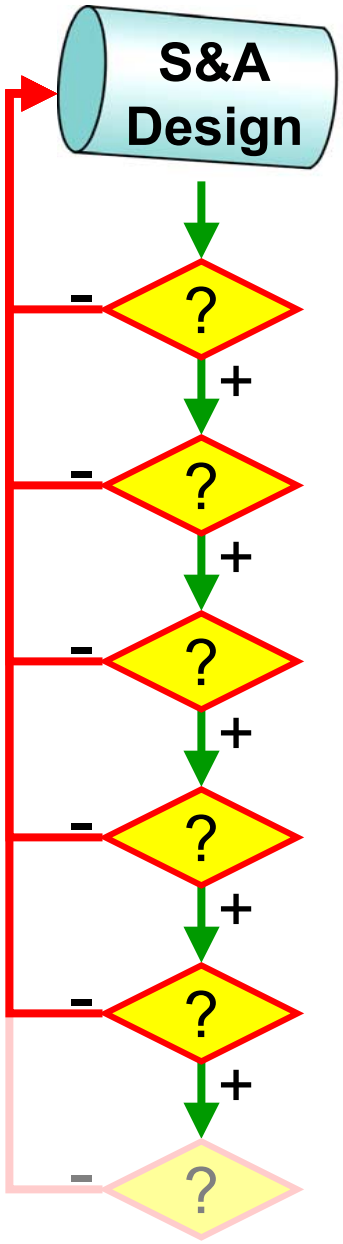
Given Parameters

- basic requirements
- interfaces
- adverse environm.
- chosen arming environments
- ...

Design Variables

- arming environments
- arming logic/sequence
- basic S&A type
- explosive train
- fail safe features
- materials/parts
- internal signal processing
- ...





S&A Design Process

1) Design can be simplified

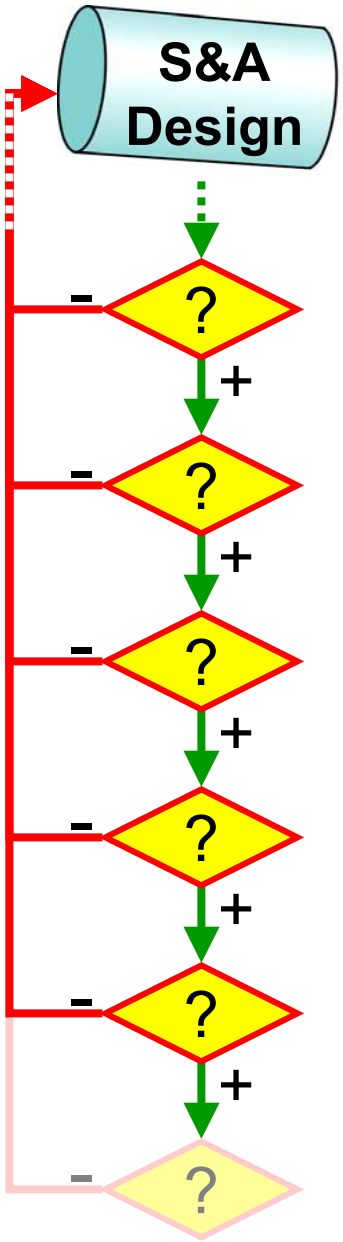
2) Design is fail safe

3) Preliminary FTA

4) Hazard Analysis

5) Sneak Circuit Analysis

6) …



S&A Design Process

6) Producability

7) Integrated Design Analysis (OL tree, …)

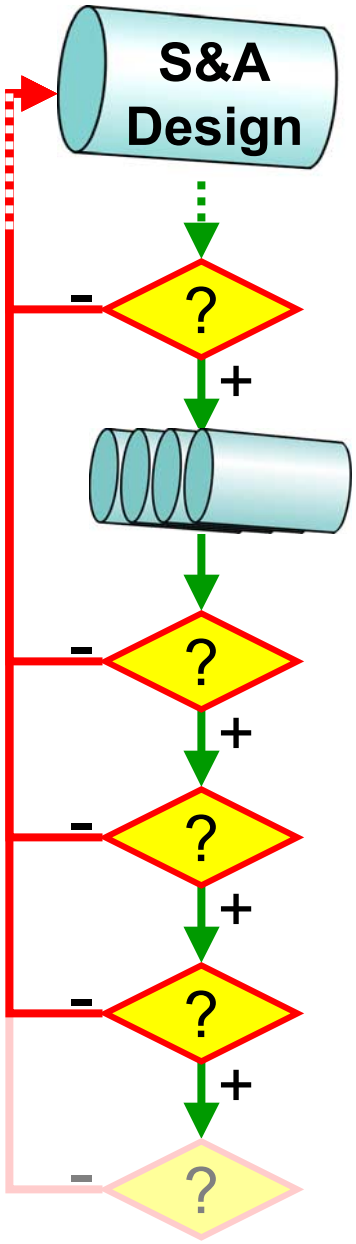
8) FME(C)A

9) FTA

10) Reliability

11) ...

S&A Design Process



11) Component Tests

Production of Test Samples

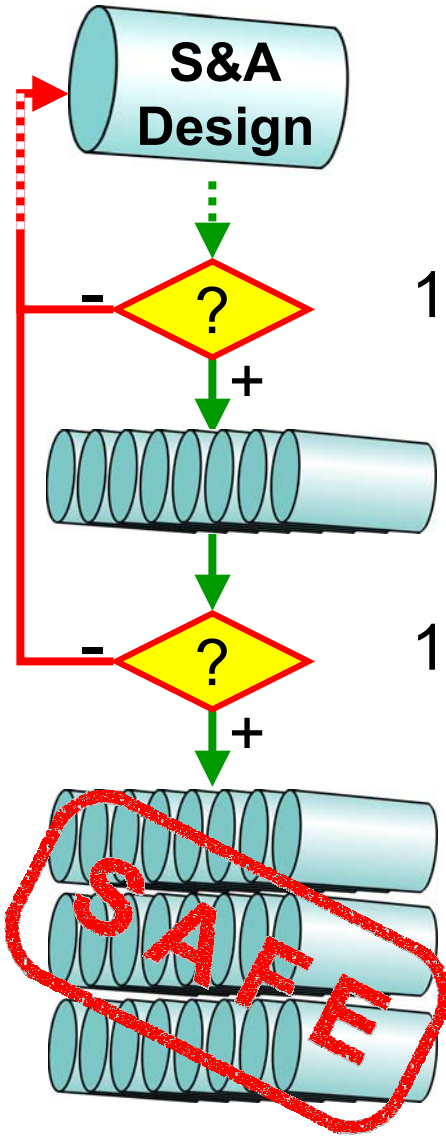
12) Function Tests

13) Qualification Level Tests

14) Test to Failure

15) ...

S&A Design Process



15) **Qualification**

Limited Production

16) User Operational Tests

Full Production

Outline

- **S&A Development Process**

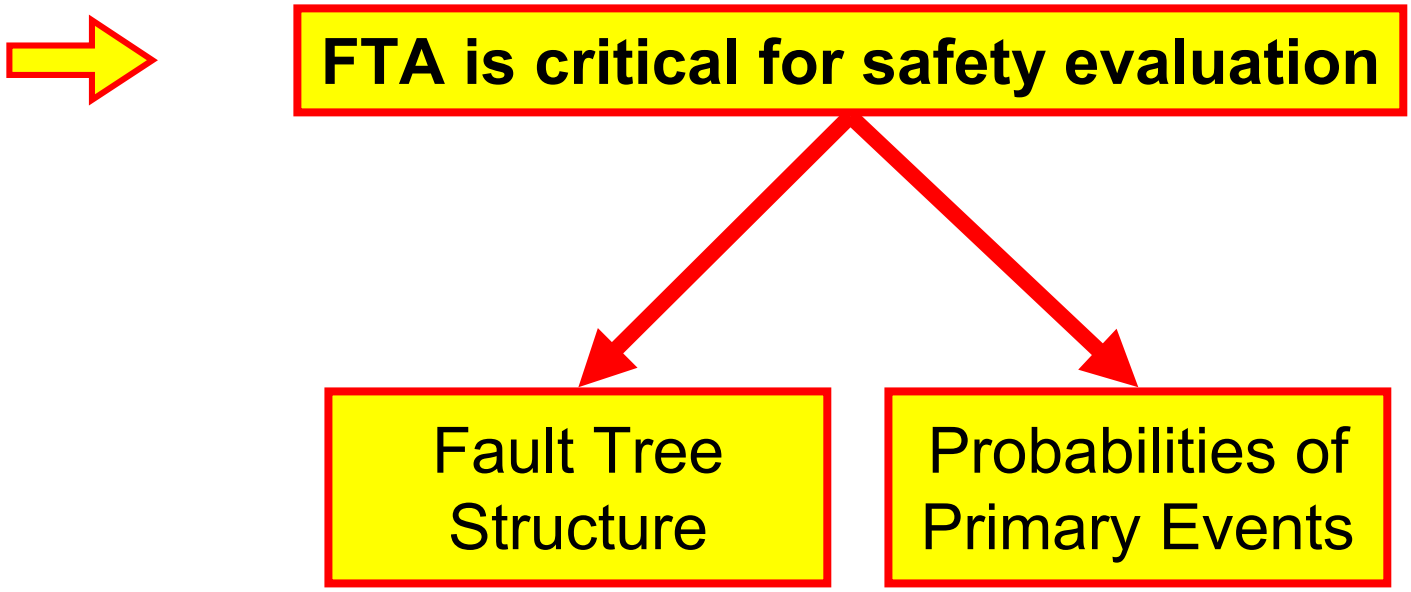
  - Steps to a safe S&A

- **Fault Tree Analysis**

  - How to do it right

Fault Tree Analysis

- FTA is basis for quantification of risk (target: $1:10^6$)



FTA - Tree Structure

- top events are Premature Arming and Early Burst
- the Fault Tree must be build on and verified at least against:
  - (P)HA
  - FME(C)A
  - drawings & schematics
  - Operation Logic Tree (from IDA)
  - SCA
- a FTA must include Primary, Secondary and Command Faults (e.g. credible accidents, errors during manufacture)

FTA - Tree Structure

- the Fault Tree should be developed into a level, where every fault from the FME(C)A and other analyses is mentioned
- subsequent deletion of limbs must be mentioned and explained

FTA - Quantitative Analysis

- provide the origin of all used data, scaling factors and expressions and explain, why they are applicable
- provide all raw data necessary to duplicate the analysis (e.g. type component, failure rate, quality level, environmental factors)
- **for ESAD** the following standard sources of failure rates should be used (as of 04/2001)

  - EPRD-97
  - NPRD-95
  - NONOP-1
  - MIL-HDBK 217(F)

FTA - Quantitative Analysis

- pooling of data:
  if - for a part only a limit of failure rate is given ("> …")
  and - for similar parts the failure rates are well defined,
  the following expression may be used for pooling (EPRD-97):

$$\lambda_{pool} = \left(\prod_{i=1}^{n'} \lambda'_i \right)^{\frac{1}{n'}} \cdot \left(\frac{\sum_{i=1}^{n'} h'_i}{\sum_{i=1}^{n} h_i} \right)$$

λ_{pool}:	resultant failure rate
λ'_i:	failure rate of part i with failure
h_i:	time of part i
h'_i:	time of part i with failure
n:	pooled parts
n':	pooled parts with failure

FTA - Quantitative Analysis

- apply a safety factor of 5 to all probabilities (to compensate for statistical uncertainties and deviations of actual parts)
- probability of failure is accumulated over all phases of weapon life cycle
  - storage (ground, field, mobile,…); Σ = 20 years
  - logistic transportation
  - mounted on weapon or A/C carriage
  - launch & flight/fall

$$P(\lambda,t) = \sum_i \lambda_i \cdot t_i$$

P : probability of failure
λ_i : failure rate in environment i
$\lambda_i = MTBF_i^{-1}$
t_i : duration of environment i

FTA - Quantitative Analysis

Example 1:

Electronic part, highly reliable but sensitive to environment

Environment	Time	λ [10^{-6}/h]	P(λ,t)	%
Ground Storage (GB)	20 yrs. = 170,265 h	0.001	$1.7 * 10^{-4}$	53
Field Storage (GF)	6 months = 4,383 h	0.01	$4.4 * 10^{-5}$	14
Transportation (GM)	21 days = 504 h	0.05	$2.5 * 10^{-5}$	8
A/C carriage (AUF)	7 days = 168 h	0.5	$8.4 * 10^{-5}$	26
Launch & Flight (ML)	120 s = 1/30 h	5	$1.7 * 10^{-7}$	0.05
			$3.2 * 10^{-4}$	

FTA - Quantitative Analysis

Example 2:

Electronic part, less reliable, less sensitive to environment

Environment	Time	λ [10^{-6}/h]	P(λ,t)	%
Ground Storage (GB)	20 yrs. = 170,265 h	0.05	$8.5 * 10^{-3}$	92
Field Storage (GF)	6 months = 4,383 h	0.1	$4.4 * 10^{-4}$	5
Transportation (GM)	21 days = 504 h	0.2	$1.0 * 10^{-4}$	1.1
A/C carriage (AUF)	7 days = 168 h	0.8	$1.3 * 10^{-4}$	1.5
Launch & Flight (ML)	120 s = 1/30 h	2	$6.7 * 10^{-8}$	0.001
			$9.2 * 10^{-3}$	

Conclusion

I have tried to show

- "Best Practice" Way of S&A Development
  - General Step-By-Step List

- "Best Practice" for FTA
  - highlighted points for FTA structure
  - guidelines for quantitative analysis

based on experiences in Germany, USA and with NATO AC/310, SG II.

Full Report available from: FowlerSE@navair.navy.mil